CLAIMS

WE CLAIM:

1. A system for providing security to a graph of interconnected nodes, the system comprising:

a grouping multiplexing layer configured to monitor calls to the system;

a graphing dynamic link layer configured to transmit data to and from the graph; and

a group security manager coupled to the grouping multiplexing layer and coupled to the graphing dynamic link layer, the group security manager configured to perform security-related acts via interacting with a group database to propagate security-related information to members of a group within the graph by controlling interactions between group members and a plurality of actions governing the group members.

2. The system of claim 1 wherein the plurality of actions includes publishing of group records, validating records that for publication, discovering group members, enabling custom roles, enabling user-defined records, and enforcing security policies.

3. The system of claim 1 wherein the group security manager generates events regarding certificates, roles and record types.

4. The system of claim 1 wherein the group security manager provides security to data published according to a graphing protocol and enables secure connections to be established between peers in the graph.

5. The system of claim 1 wherein the group security manager enables use of peer name resolution protocol to discover the group members.

6. The system of claim 1 wherein the group security manager enables peers in the graph with different capabilities to have different privileges with respect to other peers.

7. The system of claim 1 wherein the group security manager requires each node in the group to have a secure peer name.

8. The system of claim 7 wherein the secure peer name is secured via being derived from a public key that is part of a public/private key pair.

9. The system of claim 1 wherein the group security manager requires each group to have a secure peer name based on a public/private key pair.

10. The system of claim 1 wherein the group security manager requires a plurality of membership credentials to participate in the group.

11. The system of claim 10 wherein the credentials are X.509 certificates.

12. The system of claim 10 wherein credentials define privileges for the group members, the privileges including different classes of group members.

13. The system of claim 10 wherein credentials have a validity period the credentials require renewal before they expire.

14. The system of claim 12 wherein a plurality of roles define the privileges for the group members.

15. The system of claim 14 wherein each role is identified by a friendly name and a unique identifier.

16. The system of claim 14 wherein the plurality of roles have a role hierarchy that governs abilities to publish, modify and delete records.

17. The system of claim 14 the plurality of roles can include a role authorizing group members to modify one or record and authorize the group members to grant themselves privileges to perform one or more operations in the group.

18. The system of claim 1 wherein the group security manager enables secure publishing to the group database by requiring data to be published to the group to contain a cryptographic signature.

19. The system of claim 1 wherein the group security manager checks for authorization that a publisher has the right to publish each record and that a signer has the right to sign the record by checking privileges of the publisher and signer.

20. A method for a member in a group within a graph of interconnected peer nodes to renew a certificate granting privileges, the method comprising:

connecting to a second member in the group;

requesting authorization from an administrator for renewing the certificate, the renewing based on the authorization from the administrator or based on one or more security policies.

21. The method of claim 20 wherein the renewal is based on the security policies if the authorization from the administrator is not received.

22. A method for a member in a group within a graph of interconnected peer nodes to renew a certificate granting privileges, the method comprising:

receiving a request to renew the certificate that was published in a graph database; and

performing renewal according to an authorization from an administrator or based on one or more security policies.

23. The method of claim 22 wherein the renewal is performed online, the method further comprising:

contacting one or more authorized members with a shorter chain in the graph of interconnected nodes before contacting authorized members with a longer chain in the graph of interconnected nodes; and

performing one or more renewal attempts to achieve a chain that is of shorter length, wherein number of renewal attempts are proportional to length of the chain; and

if a chain is beyond a predetermined length, performing an offline renewal to shorten the chain.

24. The method of claim 22 wherein the renewal is repeated if a shorter chain can be achieved.

25. The method of claim 22 wherein more than one authorized member is the group is active, each authorized member in the group enabled to process the renewal request, the method further comprising:

providing each authorized member in the group with a random back-off prior to attempting to process the renewal request, the random back-off proportional to a length of the chain of the authorized member.

26. A method for ensuring that a publisher of information in a record to a secure group in a graph of interconnected nodes has authority to publish to the secure group, the method comprising:

creating a token for the publisher, the token containing information located in a role assigned to the publisher, the role identifying privileges of the publisher; and

matching the token against a security descriptor for the record to be published, the security descriptor providing a list of rights associated with each role.

27. The method of claim 26 wherein the token is published in a graph database, the graph database providing security related information to each member of the secure group.

28. The method of claim 27 wherein the graph database enables deferred record validation by enabling a group member to defer until required security information is available to the group member.

29. A method for revoking a member of a group of interconnected nodes within a graph, the method comprising:

publishing a revocation record to the group, the revocation record identifying the member; and

revoking any records published by the member according to the revocation record.

30. The method of claim 29 wherein the revocation record is published with validation time sufficient to ensure that a current certificate of the revoked group member expires before the revocation.

31. The method of claim 29 wherein if the member to be revoked is an administrator, the administrator privileges are first deprecated prior to the publishing the revocation record.

32. A method for revoking one or more members of a group of interconnected nodes within a graph, the method comprising:

identifying one or more bits in a revocation bit map, the bits associated with one or more serial numbers, the one or more serial numbers identifying the one or more members of the group; and

altering the one or more bits in the revocation bit map, the altering revoking the one or more members of the group.

33. The method of claim 32 wherein the revocation bit map is scalable.

34. A computer-readable medium having computer-executable instructions to perform acts for a member in a group within a graph of interconnected peer nodes to renew a certificate granting privileges, the computer-executable instructions performing acts comprising:

connecting to a second member in the group;

requesting authorization from an administrator for renewing the certificate, the renewing based on the authorization from the administrator or based on one or more security policies.

35. The computer-readable medium of claim 34 wherein the renewal is based on the security policies if the authorization from the administrator is not received.

36. A computer-readable medium having computer-executable instructions to perform acts for a member in a group within a graph of interconnected peer nodes to renew a certificate granting privileges, the computer-executable instructions performing acts comprising:

receiving a request to renew the certificate that was published in a graph database; and

performing renewal according to an authorization from an administrator or based on one or more security policies.

37. The computer-readable medium of claim 36 wherein the renewal is performed online, the computer-executable instructions further performing acts comprising:

contacting one or more authorized members with a shorter chain in the graph of interconnected nodes before contacting authorized members with a longer chain in the graph of interconnected nodes; and

performing one or more renewal attempts to achieve a chain that is of shorter length, wherein number of renewal attempts are proportional to length of the chain; and

if a chain is beyond a predetermined length, performing an offline renewal to shorten the chain.

38. The computer-readable medium of claim 36 wherein the renewal is repeated if a shorter chain can be achieved.

39. The computer-readable medium of claim 36 wherein more than one authorized member is the group is active, each authorized member in the group enabled to process the renewal request, the method further comprising:

providing each authorized member in the group with a random back-off prior to attempting to process the renewal request, the random back-off proportional to a length of the chain of the authorized member.

40. A computer-readable medium having computer-executable instructions to perform acts for ensuring that a publisher of information in a record to a secure group in a graph of interconnected nodes has authority to publish to the secure group, the computer-executable instructions performing acts comprising:

creating a token for the publisher, the token containing information located in a role assigned to the publisher, the role identifying privileges of the publisher; and

matching the token against a security descriptor for the record to be published, the security descriptor providing a list of rights associated with each role.

41. The computer readable medium of claim 40 wherein the token is published in a graph database, the graph database providing security related information to each member of the secure group.

42. The computer readable medium of claim 40 wherein the graph database enables deferred record validation by enabling a group member to defer until required security information is available to the group member.

43. A computer-readable medium having computer-executable instructions to perform acts for revoking a member of a group of interconnected nodes within a graph, the computer-executable instructions performing acts comprising:

publishing a revocation record to the group, the revocation record identifying the member; and

revoking any records published by the member according to the revocation record.

44. The computer-readable medium of claim 43 wherein the revocation record is published with validation time sufficient to ensure that a current certificate of the revoked group member expires before the revocation.

45. The computer-readable medium of claim 43 wherein if the member to be revoked is an administrator, the administrator privileges are first deprecated prior to the publishing the revocation record.

46. A computer-readable medium having computer-executable instructions to perform acts for revoking one or more members of a group of interconnected nodes within a graph, the computer-executable instructions performing acts comprising:

identifying one or more bits in a revocation bit map, the bits associated with one or more serial numbers, the one or more serial numbers identifying the one or more members of the group; and

altering the one or more bits in the revocation bit map, the altering revoking the one or more members of the group.

47. The computer-readable medium of claim 46 wherein the revocation bit map is scalable.